WiNG 5.4.2.0-030R Release Notes

Overview 1
1. Platforms Supported 2
2. New Features in WiNG v5.4.2 for RFS/NX/ AP/ ES deployments 2
3. Controller Licensing in WiNG v5.4.2 4
4. Firmware upgrade – Controllers and Dependent APs 5
4.1 Upgrade/ Downgrade Process for RFS Controllers 8
4.2 Upgrade/Downgrade of dependent APs connected to RFS controllers 10
4.3 AutoInstall 13
4.4 Full VM Upgrade for NX 45XX/ NX 65XX 13
5. Firmware upgrade & Downgrade –Independent APs 14
5.1 AP Upgrade/ Downgrade Process from WiNG v5.x to WiNG v5.x 14
5.2 Upgrade/Downgrade for AP 7131/ AP 7131N for v4.x to WiNG v5.x 15
5.3 Upgrade/Downgrade for AP 7181 from v3.2.3 to WiNG v5.4.x 16
5.4 AutoInstall 18
6. Important Notes 19

Overview

WiNG v5.4.2 continues to build on the innovative WiNG 5 architecture across the Motorola Solutions 802.11n Enterprise WLAN portfolio and provides critical fixes and enhancements for customer reported issues.
WiNG v5.4.2 is a maintenance release that introduces the following new functionality:

- 802.11r support (fast BSS transition)
- Time-based WLANs
- Aeroscout support
- Several L2TPv3 enhancements
- Support for LDAP attributes in role based firewall

Platform Support

WiNG 5.4.2 brings support for the following platforms:

- NX 4500, NX 4524, NX 6500, NX 6524
- AP 8132

Regulatory

- WiNG 5.4.2 enables FCC DFS channels and Japan DFS for AP 8132.
- WiNG 5.4.2 enables ETSI DFS channels (EN 301 893 v1.6.1) for AP 650/6532 and AP 7131/7131N for countries that follow the ETSI standards.
- AP 6562 has channel 52, 52+ and 56- shut down in this release.
- For Indonesia – only 2.4 Ghz is allowed on all AP platforms.

1. Platforms Supported

WiNG 5.4.2 supports the following platforms with the corresponding firmware images.

Controller Platform	Firmware Image
RFS 4010 / RFS 4011	RFS4000-5.4.2.0-030R.img
RFS 6000	RFS6000-5.4.2.0-030R.img
RFS 7000	RFS7000-5.4.2.0-030R.img
NX 9000 / NX 9500/ NX 9510	NX9000-5.4.2.0-030R.img
NX 45XX	NX45XX-5.4.2.0-030R.img
NX 65XX	NX65XX-5.4.2.0-030R.img

AP Platforms	Firmware Image
Dependent APs	
AP 300	01.00-2354r (included in the controller image)
AP 621	AP621-5.4.2.0-030R.img (included in the Controller image)
AP 622	AP622-5.4.2.0-030R (included in the Controller image)
AP 650	AP650-5.4.2.0-030R.img (included in the Controller image)
Independent /Adaptive APs	
AP 6511	AP6511-5.4.2.0-030R.img
AP 6521	AP6521-5.4.2.0-030R.img (included in the Controller image)
AP 6522	AP6522-5.4.2.0-030R.img (included in the Controller image)
AP 6532	AP6532-5.4.2.0-030R.img (included in the Controller image)
AP 6562	AP6562-5.4.2.0-030R.img (included in the Controller image)
AP 7131 / AP7161 / AP 7181	AP71XX-5.4.2.0-030R.img
AP 8132	AP81XX-5.4.2.0-030R.img
Independent /Adaptive Wall Switch	
ES 6510	AP6511-5.4.2.0-030R.img (ES 6510 uses AP 6511 image)

2. New Features in WiNG v5.4.2 for RFS/NX/ AP/ ES deployments

WiNG 5.4.2 introduces the following new features and functionality.

Functionality	Benefit
Wireless	
802.11r support	**IEEE 802.11r-2008** or **fast BSS transition (FT)** is a standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure handoffs from one base station to another managed in a seamless manner. 802.11r support is tested with Apple IOS 6 devices.
Time Based WLANs	WLANs can be turned on/ off at specific times of day. e.g. Guest Access can be provided during working hours only. Provides compatibility with WiNG 4.x. Available on all platforms.
Locationing with Aeroscout	Locationing support has been introduced with Aeroscout systems. Available on AP 7131N and AP 6532/ AP 650.

Functionality	Benefit
LDAP Attributes in role matching criteria	Users are granted access to the network based on active directory attributes using the Role Based Firewall. This allows the network administrator to define and use consistent roles across wired and wireless, thereby providing a unified management approach across the entire network. Note: Support is limited to Active Directory only. This feature is not supported with other LDAP servers (e.g. OpenLDAP).
Security	
Auto IPSec secure	This feature will secure the L2TPv3 control and data traffic between L2TPv3 tunnel initiator (AP / controller) and the controller / IPSec gateway. This will be a per L2TPv3 tunnel peer configuration and if enabled, then first the IPSec tunnel will be established between the L2TPv3 tunnel initiator and the controller / IPSec gateway and after this, the L2TPv3 tunnel will establishment over the IPSec tunnel.
Per VLAN firewall turn off	This feature will enable the user to disable firewall for a given vlan and hence flow table size need not be increased.
L2TPv3 client	WiNG 5.4.2 will add support for L2TPv3 client on following platforms: NX65XX, NX45XX, AP 8132, AP 6562, AP 6522, AP6521.

WiNG 5.4.2 adds following additional features for NX 45XX/ NX65XX platforms:

Functionality	Benefit
Port mirroring	Standard SPAN functionality is added to mirror packets received or sent on any of the GE ports to a destination GE port.
New Sangoma card support	Following new cards will be supported: 1. Sangoma BRI Card with EC support - B501DE Support for 2 NT ports (PSTN trunks) or 2 TE ports (ISDN desk sets) 2. Sangoma BRI Card with EC support - B502DE Support for a mix of 4 ports: 2 NT ports (PSTN trunks) and 2 TE ports (ISDN desk sets) or 4 NT or 4 TE 3. Sangoma 4FXO/1FXS with EC Card - B600DE Supports connectivity to 4 PSTN analog lines and 1 analog desk set 4. Sangoma 4FXO with EC Card - A20002DE Supports connectivity to 4 PSTN analog lines There is an issue with the partial obstruction of the top port of the following internal Telephony GW cards, GW-BR-B502DE and GW-SA-B600DE. An updated cage, KT-NXMODC-02, will be released in early Q2 2013 to address this issue

WiNG 5.4.2 adds following additional features for AP 8132 platform:

Functionality	Benefit
TPC support	AP 8132 supports Transmit Power control (802.11h). Transmit Power Control is a technical mechanism used to prevent too much unwanted interference between different wireless networks. TPC will automatically reduce the used transmission output power when other networks are within range. Reduced power means reduced interference problems and increased battery capacity.

WiNG 5.4.2 adds following additional features for AP 6562 platform:

Functionality	Benefit
Extended Radio Range	This feature is already supported on AP 7161 and AP 7181. This is the ability of the AP to provide over the air connectivity at a distance beyond the default-out-of-the-box distance. The out-of-the-box configuration defaults are as follows: – 5 GHz default range = 2 Km – 2.4GHz default range = 7Km

3. Controller Licensing in WiNG v5.4.2

Maximum Capacities of license types per controller platform	RFS4010 RFS4011	NX 45XX	RFS 6000	NX 65XX	RFS 7000	NX 9000/ NX 9500 /NX 9510
Adaptive AP Licenses applicable to: • AP 8132 • AP 71XX • AP 65XX • ES 6510 • AP 650 • AP 62X	36	72	256	264	1024	10,240 Appliance will ship with Zero ports
AP licenses Licenses applicable to: • AP8132 • AP 71XX • AP 65XX AP license • AP 650 • AP 62X • AP 300	6	AP 300 not supported	48	AP 300 not supported	256	N/A AP 300 no supported

Please note that that AP 300 continues to follow the AP license type and the AP license capacity. It is only supported by the RFS controllers.

4. Firmware upgrade – Controllers and Dependent APs

Please note that upgrading WiNG v4.x networks to WiNG v5.4.x will not retain the 4.x configuration. Please use the configuration migration utility to convert a 4.x configuration to a 5.4.x based configuration.

- *When downgrading from WiNG 5.4 to a lower version via RF domain please see Important Note 1.*
- **AP 622 v5.2.3.0-008R must be first upgraded to v5.2.3.0-040R before it can be upgraded to v.5.4.**
- Adaptive APs deployed in WiNG v4.x will retain their static IPs upon upgrade
- Controller will retain their WiNG v4.x IPs upon upgrade to 5.4.x (unlike 5.1). Basic network and port settings that are needed to establish connectivity with the switch will be retained as well, when an WiNG v4.x controller is upgraded to WiNG v5.4.x
- An offline configuration migration utility is also available as a win32 executable. The required input is a 'device generated' WiNG 4x configuration file (running-config). The output is a WiNG 5x configuration file. Please use this file as a base for your desired WiNG 5 config. Note that some functionality is not migrated – in particular, see Important Note 1.
- Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. APs connected directly to RFS 4000 and RFS 6000 controllers need the controller to stay active until the upgrade completes.
- Both the controller and the AP should be upgraded to the same versions – a firmware mismatch can cause network disruptions and should be avoided. When upgrading, the controllers should be upgraded first and then the APs. When downgrading, the APs should be downgraded first, and then the controller.
- Note: There are several changes/fixes done to SMART-RF in WiNG v 5.2 release. If upgrading to v 5.4.0 from a version prior to 5.2, execute the following commands to ensure proper SMART-RF function:
  - service smart-rf clear-config
  - service smart-rf clear-config on rf-domain
  - service smart-rf clear-history
  - service smart-rf clear-history on rf-domain.
- VPN feature has been re-implemented in WiNG 5.3 to provide a common, more optimized implementation on controllers and APs. Please use the config migration utility to migrate VPN configuration when upgrading from a WiNG 4.x release to WiNG 5.3 or higher. Please be sure to save the old VPN config. It will need to be reentered on a downgrade from v5.3 (or higher) to a WiNG 5.0.x, 5.1.x or 5.2.x releases, which don't support new VPN functionality.
- NX 45XX and NX 65XX have latest BIOS image – version 580MV112 and BIOS will be updated as part of upgrade process.
- WiNG 5.4 has support for component changes on the RFS 40XX, RFS 6000, RFS 7000 WLAN controllers. This includes NAND, Power Supervisor Chip and USB chip on the RFS6000, the NAND on the RFS 7000 and the NAND and USB on the RFS 40XX.

Support for the new NAND was introduced in release 5.2.12 on RFS 40XX, RFS 6000 and RFS 7000.

Following is the supported Upgrade/Downgrade Matrix for the various platforms

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS + AP 650/AP 300 Please see note below for further information on AP 300 upgrades	V4.3.x onwards on the controller	V4.3.x onwards on the controller	AP 650 and AP 300 images are contained within the controller image
RFS + AP 7131/AP 7131N	V4.1.1 onwards on the AP V4.3.x onwards on the controller	V4.1.1 onwards on the AP V4.3.x onwards on the controller	AP 7131/AP 7131N v5.x image is not within the controller image
RFS + AP 6532	V5.1 onwards	V5.1 onwards	AP 6532 image is contained within the controller image Note: The RFS controller would need to be upgraded to v4.3.x and then to v5.2, so that it can adopt the AP 6532
RFS + AP 6511 Controllers need to be on 5.1 to be able to adopt AP 6511.	V5.0.1 onwards, on the AP 6511 V4.3.x on the RFS to a v5.x.	V5.1 on the AP 6511 (For controller adoption, a minimum version of v5.1.x is required).	AP 6511 image is not contained within the controller image Note: The RFS controller would need to be upgraded to v4.3.x and then to v5.2, so that it can adopt the AP 6511
RFS + ES 6510 Controllers need to be on 5.4.x to be able to adopt ES 6510	5.4 and higher	5.4 and higher	ES 6510 uses the same image file as the AP 6511. The image is not contained within the controller image Note: The RFS controller would

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
			need to be upgraded to v5.4,x
RFS 4011 with AP 650 RFS 4011 are not supported on WiNG v4.x	V5.0.3/ v5.1 onwards	V5.0.3/ v5.1 Onwards	V5.0.3 only had support for AP 650s. For AP 7131 support, the minimum release required on the RFS and the AP 7131 is v5.1.
RFS /NX 9XXX + AP 7181 Controllers need to be on 5.4 to be able to adopt AP 7181.	V5.4 onwards	V 5.4 onwards	Controller assistance is not available for upgrade from 3.2.2 to 5.4. This can be performed standalone or with Wireless Manager.
RFS /NX 9XXX + AP 7161 Controllers need to be on 5.1.1 to be able to adopt AP 7161.	V5.1.1, v5.1.4, v5.2 onwards	V5.1.1, v5.1.4, v5.2 onwards	
RFS /NX 9XXX + AP 6521/ AP 621 Controllers need to be on 5.2 to be able to adopt AP 6521.	V5.2 onwards	V5.2 onwards	AP 6521 image is contained within the controller image
RFS /NX 9XXX + AP 6522 Controllers need to be on 5.4 to be able to adopt AP 6522.	V5.4 onwards	V5.4 onwards	AP 6522 image is contained within the controller image
RFS /NX 9XXX + AP 6562 Controllers need to be on 5.4.2 to be able to adopt AP 6562.	V5.4.2 onwards	V5.4.2 onwards	AP 6562 v5.x image is not within the controller image
RFS /NX 9XXX + AP 622 Controllers need to be on 5.2 to be able to adopt AP 622.	V5.2.3, V5.2.13 or 5.4 and higher.	V5.2.3, V5.2.13 or 5.4 and higher.	AP 622 image is contained within the controller image. WiNG 5.3.x does not support AP 622.

NX 45XX/ NX 65XX + AP 7131, AP 6532, AP 650, AP 6511, AP 6521, AP 621	V5.2.4, 5.4.2 and higher	V5.2.4	AP images are contained within the controller image
NX 45XX/ NX 65XX + AP 7181, AP 7161, AP 6522, AP 622, AP 6562, AP 8132	V5.4.2 and higher	V5.4.2	AP images are contained within the controller image

Notes:

- Please ensure that the controller and AP are on the same WiNG version after the upgrade is complete.
- Please be aware of the following when upgrading an AP 300 from prior images to WiNG v5.2 with an RFS controller.

Please be aware of the following when upgrading an AP 300 from prior images to WiNG v5.2 with an RFS controller.

Upgrading From	Pivot Image	Comments
WS 2000 v2.2 or prior	Please upgrade to v2.3.3 and load the Wispe image of AP 300 before plugging in the AP 300 to a WiNG v5.4.0 RFS controller.	If migrating to an RFS controller, please upgrade RFS –AP 300 to WiNG v4.3 prior to upgrading to WiNG v5.4.0.
CC-5000	If migrating to an RFS controller, please upgrade RFS –AP 300 to WiNG v4.3 prior to upgrading to WiNG v5.4.0.	A direct plug in of an AP 300 from CC-5000 to an RFS running WiNG v5.4.0 will not work. Please upgrade to pivot image of WiNG v4.3 first.
WS5100	Please upgrade to WiNG v3.3.5 or later on the RFS to v4.3, and then plug in AP 300 in to WiNG v5.4.0 – a three step upgrade.	Please ensure that WiNG v4.3 is the interim upgrade step prior to going to WiNG v5.4.0
RFS 4000/ RFS 6000/ RFS 7000	Please upgrade to WiNG v4.3 prior to upgrading to WiNG v5.4.0.	If the controller is on WiNG v4.3 or 5.1.x , then it can be directly upgraded to WiNG v5.4.0

4.1 Upgrade/ Downgrade Process for RFS Controllers

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

4.1.1 Upgrade from WiNG v5.x to WiNG v5.4.x

1. Copy the RFSX000-5.4.X.0-0XXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is —reload.

4.1.2 Upgrade from WiNG v4.3.x (or higher) to WiNG v5.4.x

1. Copy the RFSX000-5.4.X.0-0XXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is —reload.

Notes:

- When upgrading from WiNG v4.x to WiNG v5 system, the configuration is not retained or converted. Please use the configuration migration tool to convert a 4.x configuration to a 5.4.0 configuration.
- Please use ftp to upgrade to WiNG v5.4.0 on an RFS 6000, and not tftp, if using GE1.
- Due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.

4.1.3 Downgrade to a WiNG v4.3.X (or higher) from WiNG v5.4.X

1. Copy the RFSX000-4.3.X.X-XXXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<ip address of server>/<name of file>** command from CLI or **Operations>Device Detail>Load Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the Controller. From CLI the command is —reload.

Please note: due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support

new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.

4.1.4 Configuration Restoration

On upgrade from 4.x to 5.x the 5.x controller will save the configuration from 4.x in another file on flash (so that 'startup-config' will point to the 5.x default startup-config). The configuration file from 4.x is renamed to startup-config-wing4. The password encryption file is also moved to /etc2/encrypt-passwd-wing4.

On downgrade from 5.x to 4.x the controller will save the 5.x configuration and it is moved to hidden files of the same name (/etc2/.encrypt-passwd-wing5 and /etc2/nvram/.startup-config-wing5). Any previously saved wing4 config if present (ie. startup-config-wing4) is restored back.

4.2 Upgrade/Downgrade of dependent APs connected to RFS controllers

4.2.1 AP 650 upgrade

Upgrade for AP 650 from WiNG v4.x to WiNG 5.x prior to WiNG 5.4 release is seamless, and done automatically by the controller.

A WiNG 5.x controller can upgrade an AP 650 running 4.x code to 5.x using the WISPe upgrade. This capability is enabled using "legacy-auto-update" command for the controller, either under the device or profile. The controller will first adopt the access point using the standard WISPE protocol messages (just as a 4.x controller would adopt it) and then download the new image to it, which would convert the AP to WiNG 5.x version of code.
Legacy-auto-update is enabled by default. If legacy-auto-update is disabled, use the following CLI instructions to enable the Legacy-auto-update feature:

```
rfs4000-22A136#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs4000-22A136(config)#profile rfs4000 default-rfs4000
rfs4000-22A136(config-profile-default-rfs4000)#legacy-auto-update
rfs4000-22A136(config-profile-default-rfs4000)#commit
rfs4000-22A136(config-profile-default-rfs4000)#
```

Important: In WiNG 5.4.x – please enable FTP server on the controller for legacy-auto-update to work.

The AP 650 can be automatically downgraded to a 4.x version of the AP by connecting it to a controller running the version 4.x. The AP tries to discover both 4.x as well as 5.x controllers by default, and if it does not find a 5.x controller, but does find a 4.x controller, then it will adopt to it, and as part of the adoption the 4.x controller will download a 4.x image to it.

Important: Upgrade for AP 650 from WiNG 4.x to WiNG 5.4.x is NOT seamless and requires additional steps. AP 650 should first be updated to any WiNG 5.2.x or 5.3.x image.

Please set in the controller profile "service wireless ap650 legacy-auto-update-image <PATH:/ap.img> to point to WiNG 5.2.x or WiNG 5.3.x AP 650 image.

For example:

1) Copy AP650 5.2 image on the RFS flash
   rfs4000-22A1B8#copy tftp://<Server IP>/ AP650-5.2.0.0-069R.img flash:/AP650-5.2.0.0-069R.img
2) User the below command to first upgrade the AP650s to a 5.2 image
   rfs4000-22A1B8#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
   rfs4000-22A1B8(config)#self
   rfs4000-22A1B8(config-device-XXX)#service wireless ap650 legacy-auto-update-image flash:/AP650-5.2.0.0-069R.img
3) If auto upgrade is enabled AP650 will get upgraded to 5.4.1 once it adopts to the controller, else use the below command to upgrade the AP650s to 5.4.1
   rfs4000-22A1B8#ap-upgrade ap650 <DEVICE>

4.2.2 AP 7131 upgrade from AP 4.x

For AP 7131's running 4.x firmware the released 5.x firmware (AP71XX-5.4.x.0-.img) should not be used to upgrade the AP to 5.x. Instead for every 5.x release, there is a corresponding migration image to 5.x (AP7131-5.4.X.0-0XXR.bin). Please refer to section 5.2 of the release notes.

4.2.3 AP upgrade options

WiNG 5.x supports AP firmware upgrade from the controller. For firmware upgrade through controller, Firmware image needs to be loaded onto a controller and the same can be used for the upgrade of all the corresponding APs.
Available firmware on the controller can be checked using the below command:
rfs4000-22A1B8#show ap-upgrade versions

If AP firmware is not part of controller image – new image can be uploaded using following command:
rfs4000-22A1B8#ap-upgrade load-image ?
ap621 Upgrade an AP621 device
ap622 Upgrade an AP622 device
ap650 Upgrade an AP650 device
ap6511 Upgrade an AP6511 device
ap6521 Upgrade an AP6521 device
ap6522 Upgrade an AP6522 device
ap6532 Upgrade an AP6532 device
ap6562 Upgrade an AP6562 device
ap71xx Upgrade an AP71XX device
ap81xx Upgrade an AP81XX device

Once AP firmware is loaded on the controller, below are the different options that are available for AP firmware upgrade:

- **Manual Upgrade**
  Firmware upgrade can be initiated on a single or a list of Aps using the below command.
  rfs4000-22A1B8#ap-upgrade ap71xx-16C7B4 ?
  no-reboot No reboot (manually reboot after the upgrade)
  reboot-time Schedule a reboot time
  upgrade-time Schedule an upgrade time

  rfs4000-22A1B8#ap-upgrade ap71xx all ?
  no-reboot No reboot (manually reboot after the upgrade)
  reboot-time Schedule a reboot time
  upgrade-time Schedule an upgrade time

- **Scheduling Firmware upgrade**
  Firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. Firmware upgrade on the Aps follows the configured upgrade time.

  rfs4000-22A1B8#ap-upgrade all ?
  no-reboot No reboot (manually reboot after the upgrade)
  reboot-time Schedule a reboot time
  upgrade-time Schedule an upgrade time

- **Upgrade through RF Domain manager**
  Manual Firmware upgrade can be initiated through a domain manager

  rfs4000-22A1B8#ap-upgrade rf-domain default ?
  all Upgrade all access points in rf domain
  ap621 Upgrade an AP621 device
  ap622 Upgrade an AP622 device
  ap650 Upgrade an AP650 device
  ap6511 Upgrade an AP6511 device
  ap6521 Upgrade an AP6521 device
  ap6522 Upgrade an AP6522 device
  ap6532 Upgrade an AP6532 device
  ap6562 Upgrade an AP6562 device
  ap71xx Upgrade an AP71XX device
  ap81xx Upgrade an AP81XX device

4.2.4 Auto Upgrade

Auto firmware upgrade can be enabled on the controller using the below command. Once this is enabled on the controller any AP that is being adopted to the controller if has a firmware version different than what is present on the controller gets upgraded to the version present on the controller.
rfs4000-22A1B8(config-device-XXX)#ap-upgrade auto

The number of concurrent firmware upgrades can be configured using the below command based on the bandwidth available between the controller and the Aps.

rfs4000-22A1B8(config-device-XXX)#ap-upgrade count ?
<1-20> Number of concurrent AP upgrades
Note: Auto upgrade on the APs always happens through the controller.

4.3 AutoInstall

AutoInstall in v5.4.X works via the DHCP server. This requires the definition of a Motorola Vendor Class and three sub-options that can be either sent seperately, or under option 43: Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to entered as a string: —ftp://admin:motorola@192.168.1.10ll)

Option 187 - defines the firmware path and file name

Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.

DHCP vendor class for platforms is noted below:

- MotorolaRFS.RFS4000
- MotorolaRFS.RFS7000
- MotorolaRFS.RFS6000
- MotorolaNX.NX9000
- MotorolaNX.NX4500
- MotorolaNX.NX4524
- MotorolaNX.NX6500
- MotorolaNX.NX6524

4.4 Full VM Upgrade for NX 45XX/ NX 65XX

This process needs to be initiated from the WiNG CLI/UI to upgrade the VM install files in the /vmarchive partition that were installed from factory. The upgrade command is similar to what is executed when upgrading WiNG except that the image files are for specific VMs.

NX4500# upgrade tftp://<ip>/nx4500-team-VoWLAN-5.4.2.0-030R.img # This upgrades the install image files

To run the upgraded VM after the upgrade process, uninstall the running VM and install it back.
NX4500#virtual-machine uninstall team-vowlan # Uninstalls the running VM
NX4500#virtual-machine install team-vowlan # Installs the VM from the upgraded install image

Note: The VM upgrade itself will not impact the currently installed/running VM, if there is one. However as part of the uninstall process, the VM's configuration and database entries will be lost. Please be sure to export the configuration and database prior to the uninstall.

5. Firmware upgrade & Downgrade –Independent APs

When downgrading from WiNG 5.4 to a lower version via RF domain please see Important Note 1.

Following is the supported Upgrade/Downgrade Matrix for the various platforms

Independent/Adaptive Access Point	Upgrade from	Downgrade to	Notes
AP 6511	v5.0.1 v5.1 onwards	v5.1 onwards	Downgrade to 5.0.1 is not recommended
ES 6510	v5.4 onwards	v5.4 onwards	
AP 6521	v5.2.x onwards	v5.2.x onwards	
AP 6522	v5.4 onwards	v5.4 onwards	
AP 6532	v5.1 onwards	v5.1 onwards	
AP 6562	v5.4.2 onwards	V5.4.2 onwards	
AP 7131	v4.1.1 onwards	v4.1.1 onwards	
AP 7161	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	
AP 7181	v5.4 onwards	v5.4 onwards	See Note 1.
AP 8132	V5.2.6, 5.4.2 onwards	V5.2.6	

Note:

1. AP 7181 - WLAN Controller assistance is not available for upgrade from 3.2.3 to 5.4.x. This upgrade can be performed standalone or with Wireless Manager. The migration process will convert the necessary settings/configuration to maintain mesh connectivity. Please refer to section 5.3.

5.1 AP Upgrade/ Downgrade Process from WiNG v5.x to WiNG v5.x

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

5.1.1 Upgrade from WiNG v5.1.x or higher to WiNG v5.4.x

1. Copy the APXXXX-5.4.X-0XXR.img to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **AccessPoint->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the Access Point. From CLI the command is —reload.

5.2 Upgrade/Downgrade for AP 7131/ AP 7131N for v4.x to WiNG v5.x

Note: WiNG 5.1.3 added support for the new NAND for AP 7131N. WiNG 5.1.4 added support for the new NAND for AP 7161. Hardware revs with the new NAND will be unable to downgrade below these versions or version 4.1.5 – as these support the new NAND, but previous versions do not.

5.2.1 Upgrading from WiNG v4.x to WiNG v5.x

If an AP 7131 has a firmware release version 3.2.0 or earlier, it is mandatory to upgrade the access point to release version 3.2.1.0 before an upgrade to release version 4.x or later can be attempted. Users on AP 7131 release version 3.2.2 need not downgrade to version 3.2.1 and can directly upgrade to a release version 4.x or later.

Users are strongly cautioned against upgrading from the AP 7131 System Boot OS prompt. Upgrading from the Boot OS prompt is not a recommended and supported upgrade methodology on the AP 7131.

To conduct a firmware update on the AP 7131 from the run-time system software GUI:

1. Select 'System Configuration', 'Firmware Update' from the AP 7131 menu tree of the GUI.
2. Specify the name of the target firmware file within the 'Filename' field.
3. If the target firmware file resides within a directory, specify a complete path for the file within the 'Filepath (optional)' field.
4. Enter an IP address for the FTP or TFTP server used for the update.
5. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
6. Set the following FTP parameters if applicable:
    a. *Username* - Specify a username for the FTP server login.
    b. *Password* - Specify a password for FTP server login.
7. Click 'Apply'.

Click the 'Perform Update' button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update. This step may take several minutes. After this upgrade the access point will reload and come up with wing 5.x firmware.

Note: *Please use the special "migration image" (**AP7131-5.4.X-0XXR.bin**) when upgrading from 4.x to 5.x.*

If the user upgrades an AP 7131/AP 7131N running a version of code older than 4.1.1.0 using the AP migration image, there is a possibility of the AP getting "stuck" on coming up with 5.x. If this occurs, the following error message is seen on the console after bootup:

cpu not running at correct speed. Expected(500Mhz) current> Speed(600MHz)

To work-around this issue, the administrators need to type the following command after the error message: 'achip fix-cpu-speed'

When the AP comes upto runtime, upgrade again using the 'upgrade' command to the latest 5.3 release.

5.2.2 Downgrading from WiNG v5.x to AP v4.x for AP 7131/AP 7131N

To downgrade an access point running 5.x back to 4.x the reverse migration image (AP7131-5.4.X-0XXR-040105000004R.img) needs to be used. This image is installed on the AP just as a regular 5.x firmware is installed using ap-upgrade from CLI or UI. Please refer to the AP 7131 v4.1.5 release notes for downgrade to an earlier version.

Downgrade the access points using the AP-upgrade command from CLI of the AP and put all APs back to 4.x. All configurations from 5.x is lost as the AP is reverted to 4.x. However the original 4.x configuration, if any, could still be present on the AP.

5.2.3 Configuration Restore

Some of the configuration items from a 4.X AP 7131 are translated and migrated over to the 5.x version of the configuration after update. The items of configuration that are migrated are:

- Hostname
- Port phy configuration (speed, duplex)
- Port L2 configuration (trunking info)
- IP address of controller if available (translated to 'controller host' in 5.x)
- WAN interface IP addressing
- LAN interface /subnet1 IP address

If the configuration could not be read properly then the AP will come up with default 5.x configuration and create a logfile called legacyapn_<version>.dump.tar.gz in flash:/crashinfo indicating what was translated, what was the error etc, for post-analysis.

5.3 Upgrade/Downgrade for AP 7181 from v3.2.3 to WiNG v5.4.x

Note: Before AP 7181 can be upgraded to WiNG 5.4, it must be first upgraded to the migration image provided apn_03020300005MR.bin.

5.3.1 Configuration migration for AP 7181 when upgrading from v3.2.3 to 5.4.X

Only following configuration is migrated upon upgrade – network configuration, mesh point configuration and country code.

5.3.2 Network upgrade (multiple APs) using Wireless Manager v3.2.3 to 5.4.X

This scenario applies to APs that are already discovered/being managed by Wireless Manager (WM). The process involves pushing two different images to the targeted access

points. It should be noted that the firmware upgrade process in a mesh network should be conducted in an outside-in fashion. In other words, the outer most or leaf devices (devices with the most hops to a root mesh point) should be upgraded first and then moving inwards toward the root mesh point. WM supports this approach and should apply it in steps 1 and 2 below.

1. Upgrade the targeted AP 7181 devices to version v3.2.3.0-005MR via WM using " apn_03020300005MR.bin". This software is a transitional image and will prepare the device for the upgrade.
2. Upgrade the targeted AP 7181 devices (should now be running version v3.2.3.0-005MR) to version 5.4.2.0-030R via WM using "AP7181-5.4.2.0-030R.bin". This software will migrate the device from firmware v3.2.3-005MR to WiNG 5.4. The migration process will convert the necessary settings/configuration to maintain mesh connectivity. This migration process may take a few minutes to complete.
3. The migrated AP 7181 devices (now running WiNG 5.4.2.0-030R) will be able to be adopted by a controller or a virtual controller running compatible software. ***Note: These AP devices will no longer be manageable by WM.***

5.3.3 Network downgrade (multiple APs) using a RFS Controller from v5.4.x to v3.2.3

This scenario applies to APs that are already adopted by a controller or a virtual controller. It should be noted that the firmware downgrade process in a mesh network should be conducted in a outside-in fashion. In other words, the outer most or leaf devices (devices with the most hops to a root mesh point) should be upgraded first and then moving inwards toward the root mesh point. The process described below is not a purely an outside-in one but it will accommodate this approach.

1. From the adopter controller or virtual controller, upgrade the target AP 7181 devices to “AP7181-5.4.0.0-0XD-03020300005MR.img” making sure to specify the “no reboot” option associated with the upgrade in CLI/GUI. Failing to specify “no reboot” may result in the device rebooting immediately after the software is downloaded and potentially stranding one or more devices. This software will migrate the device from WiNG 5.4 firmware v3.2.3-005MR. Note: It is recommended to validate that the pushed image actually made it to the target device before proceeding to the next step.
2. After the image push is completed, restart the target devices specifying a delay appropriate for the network size. This delay is necessary to ensure that the outer devices in a mesh path receive the restart command before any intermediate devices are restarted.
3. After the restart, the migration process is completed and the targeted AP 7181 devices should be running the firmware v3.2.3-005MR. The device settings will be those which were present prior to upgrading from firmware v3.2.3-005MR to WiNG 5.4. Any configuration changes done while running the WiNG 5 image will be lost.
4. These AP devices will no longer be manageable by a WiNG 5.4 controller or a virtual controller. WM or any other entity that was used to manage these

devices while running the APN software before upgrading to MAP should be a viable option again.

5.3.4 Single AP upgrade from v3.2.3 to v5.4.X

1. Upgrade the AP 7181 to v3.2.3.0-005MR. Please ensure you have ip connectivity to ftp/tftp server
   Go to system>fw-update
   Set server <ip> (ip address of ftp/tftp server).
   Set user <username> (ftp-server user name)
   Set passwd <password>(ftp-server password)
   Set file AP 7181 to apn_03020300005MR (file name of 5MR bin image)
   Update ftp/tftp.
   Wait for a few minutes till AP 7181 comes up with 5MR build.
2. Now use "AP7181-5.4.2.0-030R.bin" to upgrade the AP 7181 to 5.4.x image.
   Go to system>fw-update
   Set server <ip> (ip address of ftp/tftp server).
   Set user <username> (ftp-server user name)
   Set passwd <password>(ftp-server password)
   Set file AP7181-5.4.2.0-030R.bin (file name of 5.4.x image)
   Update ftp/tftp.

Remember while upgrading from v3.2.3.0-005MR to 5.4.x baud rate will change from 115200 to 19200. So change the Baud rate if you see the illegible characters on console.

5.3.5 Single AP downgrade from v5.4.x to v3.2.3

Check AP 7181 has ip connectivity to ftp/tftp server.
Use following command to downgrade the AP 7181
AP7181- 1ACEAB#upgrade ftp:// <username of ftp server>:<password- of ftp server >@<ip-address of ftp server >/path /AP7181-5.4.2.0-030R-03020300005MR.img
Wait for some time - AP 7181 will downgrade to v3.2.3.0-005MR image.

Remember when downgrading baud rate will change from 19200 to 115200. So change the Baud rate if you see the illegible characters on console.

5.4 AutoInstall

AutoInstall in v5.3 works via DHCP. This requires the definition of a Motorola Vendor Class and three sub-options that can be either sent separately, or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to be entered as a string: —ftp://admin:motorola@192.168.1.10‖)
Option 187 - defines the firmware path and file name
Option 188 - defines the config path and file name
Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.

DHCP vendor class for platforms is noted below:

- MotorolaAP.AP8132
- MotorolaAP.AP7131
- For AP 7161: MotorolaAP.AP7131
- For AP 7181: MotorolaAP.AP7181
- MotorolaAP.AP6521
- MotorolaAP.AP6522
- MotorolaAP.AP6532
- MotorolaAP.AP6562
- MotorolaAP.AP6511

6. Important Notes

6.1 For new features introduced in release 5.4.2:

1. When upgrading from prior versions – new profiles for newly supported platforms will not be present in the startup-config. User can either create a default profile or do "erase startup-config".

2. Mismatch in controller and AP version (5.4.2 and below) will cause extended VLANs not to work properly.

3. Following DEMO features are not supported yet in this release:

    a. E-mail/SMS credentials for captive portal – feature will add ability to display Self Registration information and send captive portal credentials over e-mail or SMS.
    b. Time and Bandwidth Base voucher – feature will add ability to configure time (where system tracks actual time spent) or bandwidth (where system track actual bandwidth/throughput used) based vouchers for captive portal.
    c. iPass Certification – support for iPass supplicant client used for Wi-Fi access for some hotspot vendors.

4. ADSP SA cannot be run through a mesh with AP7131N tri radio; non root AP has 3rd radio as sensor

5. Interoperability with Samsung S2 devices:
   A Samsung Galaxy S2 device sometimes fails to connect using EAP-MAC authentication and WEP64 encryption. It's recommended to reduce the number of attempts (authentication eap wireless-client attempts) from default 3 to 2.

6. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.

7. ADSP Spectrum Analysis doesn't work over a mesh connection.

8. MCX max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where range is 24km.

9. Following is the DFS support in WiNG v5.4.2 for the supported radio platforms:

Product	Master DFS FCC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS ETSI	Client DFS Japan
AP 650 / 6532	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 713x	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7181	Disabled	Enabled	Enabled	Disabled	Enabled	Enabled
AP 6511	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 621 / 6521	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 622 / 6522 /6562	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8132	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
RFS 4011	Disabled	Disabled	Enabled	Disabled	Disabled	Enabled

6.2 For new features introduced in release 5.4 and 5.4.1:

1. WiNG 5.4 and above enforces the limit of policies on standalone APs. Current limit for DHCP, L2TPv3 policy and etc. is one policy per AP. When upgrading from WiNG 5.3 where the limit was not enforced – only one policy will be maintained.
2. VMM – please use following recommendations when configuring VMM feature:
   - Disable L2 Stateful Packet Inspection in Firewall Policy
   - Disable Dynamic Chain Selection on the radio
   - Use Opportunistic Rate Selection on the radio
   - Disable A-MPDU Aggregation if vehicular speed is greater than 30 mph
   - Set RTS-Threshold to 1 on all mesh devices

   Note: for more detail use case scenarios see AP 7161 VMM How-To guide.
3. It's recommended disabling IP DoS attacks in firewall policy when configuring IGMP snooping.
4. 10 GbE support on the NX 9510 is limited to SFP+ SR interfaces that are included in the controller. LR or XR SFP+ are not supported.
5. NX 9510 only supports extended VLANs in version 5.4.2. L2TPv3 tunneling, IPsec VPN, are not supported in v 5.4.2. These features will be supported in a future release.

6. When downgrading from WiNG 5.4 to a lower WiNG 5.x version through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
   ap-upgrade rf-domain <RF domain name> all no-reboot … this downgrades all APs (including the RF domain manager) without rebooting them
   reload on <RF domain name> … this reboots the entire RF domain. Staggered reboot option is not supported in this downgrade scenario.
7. The Firewall has been enhanced in 5.4 to a per-VLAN firewall which can be enabled or disabled on a per-VLAN basis. Per VLAN Firewall is enabled by default. It can be enabled using “firewall” cli command and disabled using the “no firewall” command.
8. WiNG 5.4 adds support for the new USB chip for RFS6000. Previously support was added for the new power supervisor chip.
9. Number of CRM policies is limited to 1 for AP 6511, ES 6510, AP 6521, and AP 621. Number of CRM policies is limited to 4 for AP 6522, AP 6532, AP 650, AP 71x1, AP 622 and RFS 4011.
10. There is a single profile for AP71XX. However, for AP 7161 and AP 7181 placement is set to "outdoor" at the device level. So even though the profile in the controller doesn't have the "outdoor" setting, when configuration is pushed to the AP, the outdoor placement is automatically enforced.
11. Telnet is disabled on AP 621, AP 6521, ES 6510 and AP 6511, since these have limited memory.
12. On AP 6511, AP 6521, ES 6510 or AP 621, when adopted by a controller, the GUI is disabled, to make the memory available for other core functions such as additional mint routes. It is assumed that when an AP is adopted to a controller the controllers’ GUI will be used for its configuration. To re-enable the GUI on these APs - use the “memory profile” parameter. Note that when an adopted AP (6521, 6511) or ES 6510 is separated from a controller to operate in standalone mode, the GUI will remain disabled due to this feature, unless the above command is used.

    If APs are already separated from the controller,
    a) Connect to AP CLI
    b) Set memory profile to ‘standalone’ under device override or profile context.

    If APs are currently adopted to controller then memory profile configuration change can be applied from controller CLI.
    a) Connect to Controller CLI.
    b) Set memory profile to ‘standalone’ under AP profile context.

    Changing the memory profile reboots the AP which then comes up with GUI.

    e.g. CONTROLLER(config-profile-default-ap6511)#memory-profile (adopted | standalone)

6.3 From previous releases (prior to 5.4):

1. Wireless Controller Access protocols
   - HTTPS/SSHv2/SNMP enabled by default
   - HTTP/Telnet Disabled is by default

2. Only two (2) controllers in a cluster are supported in WiNG 5.2 and higher, the same as in WiNG v5.1.x. Cluster creation changed in WiNG v5.2 as compared to WiNG v5.1.x To create a cluster, please do the following:
   a. Controller 1 needs to be fully configured and functional
   b. For controller 2 to be added:
      - Login to Controller 1. Configure "cluster name" if not already configured.
      - Log in to Controller 2, setup an SVI with a static IP address and make sure you can ping Controller 1 IP address. DHCP is not recommended for clustering since the IP address may change later on and the cluster may not form.
      - From Controller 2, execute "join-cluster <Controller 1 IP> username "admin" and the admins' password
        rfs4000-22A3DE#cluster-join 10.10.1.1 username "admin" password "motorola"
        Joining cluster at 10.10.1.1... Done
        Please execute "write memory" to save cluster configuration.

The requirement that user has to know the admin user name and pass word of Controller 1 makes sure that only the admin can add new controllers to the cluster. To make sure cluster config persists across reboots, user should do "write mem" explicitly after cluster is formed. The command "joincluster" changes only running-config, not startup-config.

3. Maximum number of clients per AP platform is as follows:

AP Platforms	Client Association Capacities
Dependent APs	
AP 300	256
AP 621	128
AP 622	256
AP 650	256
Independent AP	
AP 6511	128
AP 6521	128
AP 6522	256
AP 6532	256
AP 6562	256
AP 7131	256
AP 7161	256
AP 7181	256

The client association capacities are the same per radio/per AP.

4. Maximum number of WLANs & RF Domains supported per Platform

Controller Platform	WLAN capacity	RF Domains
NX 9000 / NX9500 / NX9510	1000	4096
RFS 7000	256	1024
RFS 6000	32	256
RFS 4010/4011	24	36

5. When using Juniper **ex2200-24p-4g** or related models when connecting Motorola Access Points – either disable IGMP snooping on the Juniper switches to ensure AP adoption or configure firewall policy filter that will allow the flow of traffic to specified destination-mac-address – 01:A0:F8:00:00:00/48.
6. If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gig E wired switch, please set link speed to 100 full, or user a GigE Power Injector.
7. Important Default Configuration Changes from 4.x to 5.x on the RFS

Description	4.x	5.x
ME1 default IP address	10.1.1.100	192.168.0.1
Auto upgrade enabled	On	On for all other platforms – controllers and AP. Disabled for the NX 9000 by default
HTTP enabled	On	Off
Default User Name/Password	admin/superuser	admin/motorola

8. APs (& ES) have a shadow or secondary IP for gaining access to the AP if the IP address of the AP is not known but the MAC address is known. To derive the shadow IP address of an AP, use the last two hex bytes of the AP's MAC address to determine the last two octets of the IP address.
   AP MAC address - 00:C0:23:00:F0:0A
   AP IP address equivalent – 169.254.240.10
   To derive the AP's IP address using its factory assigned MAC address
   a) Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.
   b) With the Calculator displayed, selct View>Scientific. Select the Hex radio button.
   c) Enter a hex byte of the AP's MAC address. For example, F0.
   d) Select the Dec radio button. The calculator converts the F0 to 240. Repeat this process for the last AP MAC address octet.
9. Default mode for a WLAN is tunnel. For Local bridging, please change config to "local bridging".

10. WLANs created using Initial Setup Wizard are not applied to the AP300 Devices. Workaround: User needs to subsequently map these wlans for AP300 devices.
11. When experiencing high number of handshake failures in AP 300 environment it's recommended to set "wpa-wpa2 handshake priority normal" in the WLAN.
12. **Features available/not available on an AP 300, when in a WiNG v5.2 or higher deployment:**
    a. It is not a site survivable Access Point, and will operate as a thin port without any mesh, local bridging or forwarding capabilities- similar to WiNG v4.x and prior releases.
    b. Roaming will work in a mixed AP environment – should be on the same L2 segment.
    c. To make bulk changes to adopted AP 300s, please use Config-AP 300 {} from the CLI.
    d. Multi-country support is available for the AP 300
    e. AP 300 is not seen as a device in the tree hierarchy, but under the controllers, when the controller is the RF Domain Manager. The AP 300 cannot be an RF Domain Manager.
    f. Sensor conversion from the controller is not supported. However, if the deployment is being upgraded, and the APs were previously converted to dedicated WIPS sensors for Air Defense WIPS, then they will continue to function as sensors.
    g. Features not supported:
        i. Unlike the other .11n APs in WiNG v5, AP 300 continues to be a thin port with all traffic being tunneled through the controller. Will not be able to locally forward traffic
        ii. L3 Mobility
        iii. SMART RF/ Self Healing
        iv. SMART Band Control will not be available
        v. No Secure WiSPe
        vi. Dual Image bank
        vii. Does not have a profile unlike the other .11n APs
        viii. Does not have the L2/L3 firewall on the AP, it resides on the controller
        ix. Sensor conversion is not available through the controller. However, if upgrading an existing installation where the AP 300 was a sensor, it would continue to be sensor, as long as it is not plugged into controller for adoption
        x. Will not support the remote packet capture like the other .11n APs in WiNG v5
13. AP adoption: APs are adopted based on valid SKUs, once discovered under the Auto provisioning policy. AP's with mismatched SKU still get adopted to the controller, but their radio does not turn on.
14. If the system flash is full from packet traces, crash files or ap-images, then there may not be enough space left on the device to create hotspot pages. If this happens, users must clear enough space from flash to allow hotspot pages to be created.

15. Radius authentication of management users uses a different configuration model from 5.0. So if upgrading from 5.0 to 5.2 or higher and you are using radius authentication for management access, you need to either change it to local authentication before upgrade, or make the mode 'fallback' and then reconfigure after upgrade using the new config model (configuring under aaa-policy).
16. Client load balancing makes decisions based on the average load in a band, in a channel within a band and average AP load. Client load balancing ignores differences in what wlans APs are beaconing. Running client-load-balancing amongst APs with different wlan config, will lead to decisions that may cause clients to NOT associate on a certain wlan
17. Install wizard is available only on the RFS 40XX, among the controller platforms.
18. In WiNG 5.x, antenna power table for the AP 650 has been updated. User should confirm power settings for the AP 650s. In 5.3, the power table for AP 6521 has been updated.
19. Multicipher support: Some of clients keep on sending deauthentication request when associated to WEP security WLAN in multicipher configuration. Please use different BSSIDs with the same WLAN, with different ciphers.
20. Commit is not allowed with radio configuration having two WLANs mapped with different data rates, as this is not a supported configuration.
21. Mesh and SMART RF – please exclude the Mesh APs from the SMART RF domain, as there may be channel changes due to RF interference that could disrupt the mesh link.
22. Air Defense sensor capabilities are supported on all the 802.11n APs in this release, and are available for enabling the WIPS functionality as well as the Network Assurance Capabilities. There are some caveats on managing the AP directly via ADSP, for certain AP platforms:

Network Assurance Toolset when Radio is dedicated as a sensor	**AP 621 651 6521** (Note 1)	**AP 650**	**AP 622**	**AP 6532**	**AP 6522 6562**	**AP 7131 7161 7181**	**AP 8132**
Spectrum Analysis	No	Yes	No	Yes	No	Yes	No
Advanced Spectrum Analysis	Yes	No	Yes	No	Yes	No	Yes
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Live View	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note 1: GUI is disabled and number of SSH sessions is limited to 1

23. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is available on all the 802.11n APs with some caveats – please see details below:

Network Assurance Toolset with Radio Share	**AP 6511 621 6521** (Note 1)	**AP 650**	**AP 622**	**AP 6532**	**AP 6522 6562**	**AP 7131 7161 7181**	**AP 8132**
Spectrum Analysis	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No (Note 2)	No
Advanced Spectrum Analysis	Yes	No	Yes	No	Yes	No	Yes
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Live View	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note 1: GUI is disabled when Radio Share is enabled
Note 2: Spectrum Analysis is not supported with Radio share enabled.

24. VPN feature has been re-implemented in WiNG 5.3 to provide a common, more optimized implementation on controllers and APs. Please use the config migration utility when upgrading from a WiNG 4.x release to WiNG 5.4.0. It is recommended that you save your old VPN config to assist in possible downgrades. Please see Note 2 on which VPN configurations cannot be converted using the migration utility, as they are not supported in 5.3. In particular, note that configurations containing AH and DES as IKE encryption algorithm cannot be migrated. For upgrades from WiNG 5.1.x or 5.2.x to WiNG 5.4.0, the VPN config migration is performed automatically (tool is not required).
25. IPsec VPN – In comparison to VPN implementation on RFS controllers on WiNG 4.x or WiNG v5.x, here are the primary differences.
    a. Authentication Header (AH) is not supported in v5.x, but was supported in WiNG 4.x VPN. Use ESP instead of AH.
    b. L2TP over IPsec is not supported in v5.x, but was supported in WiNG4.x VPN. WiNG 5.x supports XAUTH and can be used with a IPsec VPN clients. XUATH has been tested with Cisco and Safenet VPN clients.
    c. IKEv2 was not supported in WiNG 4.x, but is supported in WiNG 5.x.
    d. DES encryption is not supported in the IKE proposal.
    e. Transport mode is only supported for host-to-host rule, in other cases it will fall back to Tunnel mode.
    f. Transport mode NAT-Traversal not supported for IKEv1 and IKEv2 in 5.x. This is supported in tunnel mode.
    g. In the case of IKEv1, if PFS option for IPSec SA (under crypto map entry) is configured on both peers, then the value requested by the initiator is used for

the tunnel. If the configured PFS value on the initiator end is lower than that configured on the responder, the lower value is used. If PFS is required, please configure the same PFS value in both the peers.

h. The value of Kilobyte expiry of an IPSec SA (security-association lifetime kilobytes) can be configured to as low as 500KB. This has to be used with caution. If there is a lot of traffic on the tunnel and the value is set to very low value, the tunnel will end up in an indefinite rekeying IPSec SA state. This value has to be arrived at based on the maximum traffic that is expected on the tunnel and set such that there is an interval of at least a few minutes between rekeys. It is recommended that this value be set to a minimum of 512000 (500MB).
Impact from lack of the above 4.x features if any, is expected to be minimal.

26. IPsec VPN statistics - following SNMP tables are not available for VPN statistics via SNMP – they will be implemented in a future release – wingStatsDevVpnIpsecSaTable, wingStatsDevVpnIpsecSaTrafficSelectorTable, wingStatsDevVpnIkesaTable

27. Built-in RADIUS server is available as a demo capability on AP 6521 and can be configured via CLI.

28. Auto-tunnel for VPN
    a. A single group id/PSK is supported on RFS controllers. All APs use same group id/ PSK.
    b. When APs are behind NAT (e.g. two remote sites), it is required that the AP IP address are different.
    c. Auto IPsec tunnel termination has been verified on Cisco Gateways with PSK/RSA authentication.

29. VRRP
    a. VRRP version 3.0 (RFC 5798) and 2.0 (RFC 3768) are supported. Default is version 2 to support interoperability. Please note that only version 3 supports sub-second failover.
    b. Services like DHCP, RADIUS, NAT, and VPN running on the virtual IP are supported
    c. For DHCP relay, you can point to the DHCP server as virtual IP
    d. For VPN, on the initiator side, remote peer can be configured as virtual IP

30. If using TFTP to upgrade an AP 6521, AP 6511, ES 6510 or AP 621, on the TFTP server please configure the following settings:
    a. Per packet timeout in seconds: 15
    b. Maximum retries: 20

31. When using iPods as clients, you may see WPA2 group key rotation handshake failures while MUs are idle (2.4GHz band). Change the handshake timeout to 2 sec to correct this problem. From the wlan config, the cli command is: wpa-wpa2 handshake timeout X (where X is the timeout in ms, within a range of 10-5000)

32. Auto assign sensor is not available for AP 6511, AP 6521, ES 6510 or AP 621 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.

33. For IGMP Snooping version v2, v3, source specific multicast is not supported, this will be addressed in a future release.
34. To safeguard against unknown attacks, it is recommended that management access be restricted to authorized hosts/ subnets. This can be done using the restrict-mgmt-access host/subnet cli command under management-policy.
35. RFS 7000 - Compact flash card will not work on pre-Rev F RFS 7000 hardware.
36. NX 9XXX:
    - NX 9000 requires a laptop with a minimum of 4GB RAM for viewing GUI with greater than 3000 AP.
    - Extended VLANs are not supported on the NX 9000/ NX 9500. Only Local VLANs are supported.
    - There is no VPN, or Advanced WIPS support on the NX 9000/ NX 9500.
37. AP 7131: PoE and Gigabit Ethernet Ports:

    The AP 7131 family features upgraded Gigabit Ethernet (GE) ports. These ports are labeled as follows:

    - GE1/ PoE: GE1 is the LAN Port and supports 802.3af, 802.3at (draft) PoE.
    - GE2: GE2 is the WAN port.

    Single radio models can operate fully with 802.3af power sources. Dual radio models and tri-radio models can also power up two radios and GE1 interface with 802.3af power sources. At higher power levels, 2 radios and both Ethernet interfaces are fully functional in the dual and tri-radio models. Single, dual and tri-radio models can also operate using an A/C power supply. The third radio (dedicated WIPS sensor radio or a future modular off-the-shelf 3G WAN Express Card) on the tri-radio model requires 802.3at power levels, A/C power supply or a Gigabit Ethernet PoE+ injector.

The following table shows the radio and LAN resources available under various power configuration modes for the AP 7131 family:

Available Power	**Radio Resources**	**Ethernet Port Configuration**
Power Status: 3af (12.95W)	2 Radios	GE1 10/100/1000
Power Status: 3at (24W)	3 Radios (Express Card option supported with radios at lower power)	GE1 10/100/1000 GE2 10/100/1000
Power Status: Full Power (30W)	3 Radios (with Express Card)	GE1 10/100/1000 GE2 10/100/1000

When a Motorola 802.3af power injector (AP-PSBIAS-1P2-AFR) is used with AP- 7131 or AP 7131N, then the GE1 or LAN1 port will be limited to 10/100 Mbps. Motorola

recommends the 802.3at (Draft) power injector (AP-PSBIAS-1P3-AFR) to be used with AP 7131/AP 7131N configurations.

MOTOROLA SOLUTIONS and the Stylized M Logo are
registered in the US Patent & Trademark Office.
© Motorola Solutions, Inc. 2013. All rights reserved.